JOURNAL OF ALGEBRA 90, 556–566 (1984)

Counting Modular Irreducible Characters

GEOFFREY R. ROBINSON

Department of Mathematics, University of Chicago, Chicago, Illinois 60637

Communicated by Walter Feit

Received March 8, 1983

In this paper, we will be concerned with the following question: given a finite group G, a prime divisor p of $|G|$, and a p-subgroup D of G, how many modular irreducible characters of G lie in p-blocks whose defect group is D? We will give a description of this number as the difference between the ranks of two matrices with entries in $GF(p)$. We will also discuss how the methods we describe can be used to compute the number of modular irreducible characters in a specific p-block whose defect group is (contained in) D.

From now on, then, G, p and D are fixed. Let $\{y_i : 1 \leqslant i \leqslant m\}$ be a full set of representatives for the conjugacy classes of p-regular elements of G. For each i, let Q_i be a fixed Sylow p-subgroup of $C_G(y_i)$, and choose y_i and Q_i wherever possible so that $Q_i \leqslant D$. Label so that $Q_i \leqslant D$ for $1 \leqslant i \leqslant r$, but no conjugate of Q_i is contained in D for $i > r$.

DEFINITION. We say that y_i is *distinguished* if, for some $P \in \mathrm{Sylp}(G)$, we have: $P \cap P^{y_i} = Q_i$ and $N_P(Q_i) \in \mathrm{Sylp}(N_G(Q_i))$.

Remark. This definition is independent of the particular conjugate chosen from the class of y_i, and of the particular Sylow p-subgroup of $C_G(y_i)$ chosen. We also remark that the above conditions imply that $N_{Py_i}(Q_i) \in \mathrm{Sylp}(N_G(Q_i))$, so that $P \cap P^{y_i}$ is a tame Sylow intersection, and $Q_i = O_p(N_G(Q_i))$.

We relabel, if necessary, so that y_i is distinguished for $1 \leqslant i \leqslant n$, but y_i is not distinguished for $n < i \leqslant r$.

DEFINITION. For $1 \leqslant i, j, k \leqslant m$, we define the set $\Omega_{ij}^{(k)}$ to be: $\{(a, b) : a$ is conjugate to y_i, b is conjugate to y_j, and $a^{-1}b \in y_k Q_k\}$. We note that Q_k acts by conjugation on $\Omega_{ij}^{(k)}$ for any i, j, and that the length of the orbit containing (a, b) is $[Q_k : Q_k \cap C_G(a) \cap C_G(b)]$. Thus $(|Q_j|/|Q_k|)\,|\Omega_{ij}^{(k)}$ is an integer (as b is conjugate to y_j).

For $1 \leqslant k \leqslant r$, we define the $n \times r$, matrix $A^{(k)}$, with entries in $GF(p)$, by:

0021-8693/84 $3.00

$a_{ij}^{(k)}$ is the residue (mod p) of $(|C_G(y_j)|/|C_G(y_k)|)\,|\Omega_{ij}^{(k)}|$ (the latter expression is not an integer, but *is* a p-adic integer) for $1 \leqslant i \leqslant n$, $1 \leqslant j \leqslant r$.

We define the $rn \times r$ matrix $A(D)$ to be the matrix whose $(tn+i)$th row is the ith row of the matrix $A^{(t+1)}$ for $0 \leqslant t \leqslant r-1$ and $1 \leqslant i \leqslant n$.

We define the matrix $A_0^{(k)}$ in a similar fashion to $A^{(k)}$, for those k for which $Q_k < D$, except that its rows are indexed by those distinguished y_i for which $Q_i < D$, and its columns are indexed by those y_j for which $Q_j < D$. We then define the matrix $A_0(D)$ in a manner analogous to that in which $A(D)$ was defined.

THEOREM 1. (a) *The total number of modular irreducible characters in p-blocks of G whose defect groups are contained in D is the rank of the matrix $A(D)$.*

(b) *The total number of modular irreducible characters in p-blocks of G with defect group D is* $\operatorname{rank}(A(D)) - \operatorname{rank}(A_0(D))$.

We defer the proof of Theorem 1 for the moment. The following lemma allows us to reduce the computations involved (from now on, the notation $A \lesssim B$ means: "A is conjugate to a subgroup of B").

LEMMA 2. (i) $a_{ij}^{(k)} = 0$ *unless* $Q_j \lesssim Q_k$, *and* $O_p(N_G(Q_j)) \lesssim Q_i$.

(ii) *The rank of the matrix $A(D)$ (and similarly $A_0(D)$) is unchanged if we replace $a_{ij}^{(k)}$ by 0 whenever $Q_k \not\lesssim Q_i$.*

We defer the proof of Lemma 2. If $D \notin \operatorname{Sylp}(G)$, then $y_k \neq 1_G$ for $1 \leqslant k \leqslant r$, and we may as well label so that $y_m = 1_G$. The sets $\Omega_{ij}^{(m)}$ have special importance for our work. We define the $n \times r$ matrix $S(D)$ to have (i,j)-entry s_{ij}, where s_{ij} is the residue (mod p) of $(|C_G(y_j)|/|G|\,|\Omega_{ij}^{(m)}|$ (for $1 \leqslant i \leqslant n$, $1 \leqslant j \leqslant r$). (If $D \in \operatorname{Sylp}(G)$ and we label so that $y_m = 1_G$, then $S(D)$ is the matrix $A^{(m)}$).

THEOREM 3. (i) *From a knowledge of the matrix $S(D)$, it is possible to determine which subgroups of D are defect groups for p-blocks of G.*

(ii) *From a knowledge of the matrices $S(D)$ and $A(D)$ it is possible to determine all primitive idempotents of $I(D)$, and to determine the number of modular irreducible characters in each p-block of G with defect group contained in D.*

Proof of Theorem 1. Let w be a primitive $|G|_{p'}$-th root of unity, and let $K = \mathbb{Q}(w)$. Let R be the localization at a prime ideal, containing p, of the ring of algebraic integers of K. Let π be the unique maximal ideal of R, let $F = R/\pi$, and let $*$ denote images in F of elements of R.

Let $I(D)$ denote the ideal of $Z(FG)$ which is spanned as a vector space by

class sums of classes whose defect groups are contained up to conjugacy in D. Let K_i be the class sum of the class of y_i, and let $I^*(D)$ denote the subspace of $Z(FG)$ spanned by $\{K_i : 1 \leqslant i \leqslant r\}$. Let $\{e_i : 1 \leqslant i \leqslant q\}$ be the set of primitive idempotents of $Z(FG)$, and let λ_i be the linear character of $Z(FG)$ afforded by e_i for $1 \leqslant i \leqslant q$.

As in [1], we define the algebra endomorphism $s: Z(FG) \to Z(FG)$ by $Xs = \sum_{i=1}^{q} \lambda_i(X)e_i$. Then $s^2 = s$, $\ker(s) = \mathrm{rad}(Z(FG))$, and $Z(FG)s$ is the largest semi-simple subalgebra of $Z(FG)$. As in [1], it follows that Xs is a power of X for each $X \in Z(FG)$, so that s leaves every subalgebra and ideal of $Z(FG)$ invariant. We also note that, for any X,

$$(Xs)^{|F|} = \sum_{i=1}^{q} \lambda_i(X)^{|F|} e_i = \sum_{i=1}^{q} \lambda_i(X) e_i = Xs.$$

For $x \in G$, and an irreductible character χ of G, we have $|G: C_G(x)|$ $(\chi(x)/\chi(1)) \in \pi$ unless x centralizes a defect group of the p-block of G which contains χ. If X is the class sum of the class of x in $Z(FG)$, Xs is a linear combination of idempotents, all of which are in p-blocks whose defect groups are contained up to conjugacy within $C_G(x)$. Hence $I(D)s$ is spanned by primitive idempotents of $Z(FG)$ contained within $I(D)$. Thus $\dim_F(I(D)s)$ is precisely the number of p-blocks of G whose defect groups are contained in D.

We first prove that the number of modular irreducible characters in p-blocks of G whose defect groups are contained in D is the dimension of the space spanned by $\{(K_i s)K_j : 1 \leqslant i \leqslant n,\ 1 \leqslant j \leqslant r\}$.

Let $Z_0(FG)$ denote the subspace of $Z(FG)$ which is spanned by the class sums of classes of p-regular elements. We first note that $Z_0(FG) = \bigoplus_{i=1}^{q} e_i Z_0(FG)$ (as vector space). Since $e_i e_j = 0$ when $i \neq j$, it is only necessary to prove that $e_i Z_0(FG) \subseteq Z_0(FG)$ for each i. Let E_i be the unique idempotent inverse image of e_i in $Z(RG)$, and let $\hat{X}$ be the class sum in RG of the class containing the p-regular element x. Let B_i be the p-block of G which contains e_i.

For any $w \in G$, the coefficient of w in the product $E_i \hat{X}$ is $(1/|C_G(x)|) \sum_{\chi \in B_i} \chi(x)\overline{\chi(w)}$, which is 0 unless w is p-regular, by the usual block orthogonality relation. Thus $E_i Z_0(RG) \subseteq Z_0(RG)$ (where $Z_0(RG)$ is the obvious analogue of $Z_0(FG)$), so that $e_i Z_0(FG) \subseteq Z_0(FG)$, as claimed.

We next claim that for $1 \leqslant i \leqslant q$ the number of modular irreducible characters in B_i is precisely $\dim_F(e_i Z_0(FG))$. It is only necessary to prove that the number of such characters is at least $\dim_F(e_i Z_0(FG))$, since we know that $\sum_{i=1}^{q} \dim_F(e_i Z_0(FG)) = \dim_F(Z_0(FG)) =$ number of p-regular conjugacy classes of G = number of modular irreducible characters of G.

For $\hat{X}, E_i, x$ and w as above, we saw that the coefficient of w in $E_i \hat{X}$ was given by: $(1/|C_G(x)|) \sum_{\chi \in B_i} \chi(x)\overline{\chi(w)}$. It quickly follows that the rank of the

R-module $E_iZ_0(RG)$ is at most $\mathbb{C}$ rank $(U_i\bar{U}_i^T)$, where U_i is the matrix with typical entry $\chi(y)$, as χ ranges through irreducible characters in B_i and y ranges through representatives of the conjugacy classes of p-regular elements of G.

Now $\dim_F(e_iZ_0(FG)) = \text{rank}_R(E_iZ_0(RG)) \leqslant \mathbb{C}\text{-rank}(U_i)$, and it is well-known that $\mathbb{C}$-rank(U_i) is precisely the number of modular irreducible characters in B_i. It follows, then, that $\dim_F(e_iZ_0(FG))$ is just the number of modular irreducible characters in the block B_i.

(No doubt this is a well-known fact, but its proof was included for the sake of completeness.)

We next claim that $e_iZ_0(FG) = e_iI^*(D)$ whenever the defect group of B_i is contained in D. Let X be the class sum of a class of p-regular elements of G, and suppose that the defect group of B_i is contained in D. Then $e_i \in I(D)$, $e_i(e_iX) = e_iX$, and $e_iX \in Z_0(FG) \cap I(D)$ (for $I(D)$ is an ideal). Thus $e_iX \in I^*(D)$, and $e_iX(=e_i^2X)) \in e_iI^*(D)$. Hence $e_iZ_0(FG) = e_iI^*(D)$.

We relabel (of necessary), so that $\{e_i : 1 \leqslant i \leqslant t\}$ is the set of block idempotents from p-blocks of G whose defect groups are contained in D. The total number of modular irreducible characters in p-blocks of G whose defect groups are contained in D is then given by $\sum_{i=1}^{t} \dim_F(e_iI^*(D)) = \dim_F(I(D)s\, I^*(D))$.

We now prove that $I(D)s$ is spanned by $\{K_is : 1 \leqslant i \leqslant n\}$, from which it will quickly follow that $I(D)s\, I^*(D)$ is spanned by $\{K_isK_k : 1 \leqslant i \leqslant n, 1 \leqslant k \leqslant r\}$.

For $1 \leqslant j \leqslant r$, K_js is a power of K_j, so that K_js lies in the ideal $I(Q_j)$ (the obvious analogue of the ideal $I(D)$) and, as K_js is a linear combination of idempotents, K_js is a linear combination of $K_1, K_2, \ldots, K_r$. We claim that if K_k appears with non-zero coefficient in K_js and $|Q_k| = |Q_j|$ then y_j is distinguished (and, furthermore, Q_j is a defect group for some p-block of G).

Let τ denote the Brauer homomorphism from $Z(FG)$ to $Z(FN_G(Q_j))$, and suppose that K_k appears with non-zero coefficient in K_js, and that $|Q_k| = |Q_j|$. Since $K_js \in I(Q_j)$, Q_k is conjugate to Q_j. Thus $K_j\tau$ and $K_k\tau$ are single class sums within $Z(FN_G(Q_j))$. Now $(K_js)\tau = (K_j\tau)s'$, where s' is the map analogous to s, but from $Z(FN_G(Q_j))$ to $Z(FN_G(Q_j))$.

Let $K_js = \lambda_kK_k + Y$, where Y does not involve K_k. Then $(K_j\tau)s' = (K_js)\tau = \lambda_k(K_k\tau) + Y\tau$, and $Y\tau$ does not involve $K_k\tau$. By Theorem 1 of [1], Q_j is a defect group for some p-block of $N_G(Q_j)$, so for some p-block of G (for in the notation of [1], $s_{jk} \neq 0$). By the same theorem, for $P_j \in \text{Sylp}(N_G(Q_j))$, there is a conjugate z, of y_j such that $P_j \cap P_j^z = Q_j$. Replacing P_j by a suitable conjugate if necessary, we may suppose that $z = y_j$.

Let P be a Sylow p-subgroup of G with $P_j \leqslant P$. A standard argument tells us that $P \cap P^{y_j} = Q_j$. Also, $N_p(Q_j) = P_j \in \text{Sylp}(N_G(Q_j))$, so that y_j is distinguished, as claimed.

Suppose that $\{K_i s: 1 \leqslant i \leqslant n\}$ does not span $I(D)s$. Then we may choose K_j such that $K_j s$ does not lie in the span of the above set with $j \leqslant r$, and with $|Q_j|$ minimal subject to these conditions. Let $K_j s = \sum_{k=1}^{r} a_{jk} K_k$. Since $K_j s$ is a power of K_j, whenever $a_{jk} \neq 0$ we have $Q_k \lesssim Q_j$. Suppose that $|Q_k| < |Q_j|$ whenever $a_{jk} \neq 0$. Then as $s^2 = s$, we have $K_j s = \sum_{k=1}^{r} a_{jk}(K_k s)$, and by the minimality of $|Q_j|$ we see that $K_k s$ is in the space spanned by $\{K_i s: 1 \leqslant i \leqslant n\}$ whenever $a_{jk} \neq 0$. This is a contradiction, as $K_j s$ does not lie in this space.

Thus for some k with $a_{jk} \neq 0$, $|Q_k| = |Q_j|$. By our earlier argument, y_j is distinguished, so $j \leqslant n$ already, contrary to the fact that $K_j s$ does not lie in the space spanned by $\{K_i s: 1 \leqslant i \leqslant n\}$.

This contradiction establishes that $\{K_i s: 1 \leqslant i \leqslant n\}$ does span $I(D)s$, as claimed, and consequently $\{(K_i s)K_k: 1 \leqslant i \leqslant n, 1 \leqslant k \leqslant r\}$ spans $(I(D)s)I^*(D)$. The proof of Theorem 1 can now be completed by using elementary linear algebra and the following lemma.

LEMMA 4. *For* $1 \leqslant i, j, k \leqslant r$, $(K_i s)K_k = \sum_{j=1}^{r} a_{ij}^{(k)} K_j$.

Proof. We first note that $K_i s \in I(D)$, so that $(K_i s)K_k \in I(D)$. Furthermore, $(K_i s)K_k$ is a linear combination of terms of the form eK_k, where e is an idempotent, so that $(K_i s)K_k$ involves only p-regular class sums, and is a linear combination of $K_1, K_2, \ldots, K_r$.

For $1 \leqslant j \leqslant r$, $a_{ij}^{(k)}$ is the residue (mod p) of $(|C_G(y_j)|/|C_G(y_k)|)\,|\Omega_{ij}^{(k)}|$. From the well-known formula of Burnside, it can quickly be seen that

$$|\Omega_{ij}^{(k)}| = \frac{|G|}{|C_G(y_i)|\,|C_G(y_j)|} \sum_{\chi \in \mathrm{Irr}(G)} \frac{\overline{\chi(y_i)}\chi(y_j)}{\chi(1)} \sum_{x \in Q_k} \overline{\chi(y_k x)}.$$

Let $\chi^{(k)}$ denote the class function of Q_k defined by: $\chi^{(k)}(x) = \chi(y_k x)$ for each $x \in Q_k$. As $y_k \in C_G(Q_k)$, it is easy to see that $\chi^{(k)}$ is an algebraic integer combination of irreducible characters of Q_k for each $\chi \in \mathrm{Irr}(G)$.

Rearranging our earlier equation, and taking residues in F gives

$$a_{ij}^{(k)} = \left(\frac{|Q_k|}{|C_G(y_k)|} \sum_{\chi \in \mathrm{Irr}(G)} \frac{|G: C_G(y_i)|\chi(y_i)}{\chi(1)} \overline{\chi(y_i)}\,(\chi^{(k)}, 1)_{Q_k} \right)^*,$$

so that

$$a_{ij}^{(k)} = (|C_G(y_k)|_{p'}^*)^{-1} \sum_{b=1}^{q} \lambda_b(K_i) \sum_{\chi \in B_b} \overline{\chi(y_j)}^*\,(\chi^{(k)}, 1)_{Q_k}^*.$$

For $1 \leqslant b \leqslant q$, and for any $u \in Q_k^{\#}$, we have: $\sum_{\chi \in B_b} \overline{\chi(y_j)}\chi(y_k u) = 0$, since $y_k u$ is p-singular and y_j is p-regular. From this it follows that

$$\frac{1}{|C_G(y_k)|_{p'}} \sum_{\chi \in B_b} \overline{\chi(y_j)}\,(\chi^{(k)}, 1)_{Q_k} = \frac{1}{|C_G(y_k)|} \sum_{\chi \in B_b} \overline{\chi(y_j)}\chi(y_k),$$

which is the coefficient of $\hat{K}_j$ the product $\hat{K}_k E_b$ (where $\hat{}$ denotes images in $Z(RG)$, and E_b is the unique idempotent inverse image of e_b in $Z(RG)$).

Hence $a_{ij}^{(k)} = \sum_{b=1}^{q} \lambda_b(K_i)$ (coefficient of K_j in $K_k e_b$), which is just the coefficient of K_j in $(\sum_{b=1}^{q} \lambda_b(K_i)e_b)K_k$. This last expression is precisely $(K_i s)K_k$, so that $(K_i s)K_k = \sum_{j=1}^{r} a_{ij}^{(k)} K_j$, as claimed. This completes the proof of Lemma 4 and Theorem 1 (we have only given an explicit proof of part (a) of Theorem 1; an examination of the proof should convince the reader that the rank of the matrix $A_0(D)$ is the number of modular irreducible characters in p-blocks of G whose defect groups are *strictly* contained in D, and then part (b) quickly follows).

Proof of Lemma 2. (ii) We claim that if $Q_k \not\lesssim Q_i$ then $(K_i s)K_k$ is already in the space spanned by $\{(K_i s)K_j : Q_j \lesssim Q_i \text{ and } j \leqslant r\}$. Since $(K_i s)^{|F|} = K_i s$, we have: $(K_i s)K_k = (K_i s)(K_i s)^{|F|-1}K_k$. Now $(K_i s)^{|F|-1}K_k$ is a linear combination of class sums K_j for which $j \leqslant r$ and $Q_j \lesssim Q_i$ (for $(K_i s)^{|F|-1}K_k \in I(Q_i)$, and involves only p-regular class sums). Thus $(K_i s)K_k$ is in the space that we claimed it was.

(i) We have seen that $a_{ij}^{(k)}$ is the coefficient of K_j in the product $(K_i s)K_k$. Let τ denote the Brauer homomorphism from $Z(FG)$ to $Z(FN_G(Q_j))$, and let s' denote the map from $Z(FN_G(Q_j))$ to $Z(FN_G(Q_j))$ which is the obvious analogue of the map s.

Since $K_j\tau$ is a single class sum within $Z(FN_G(Q_j))$, $a_{ij}^{(k)}$ is also the coefficient of $K_j\tau$ in $(K_i s)\tau(K_k\tau)$. Now $(K_i s)\tau = (K_i\tau)s'$. Now when X is the class sum of a class of $N_G(Q_j)$, $X \in \mathrm{rad}(ZFN_G(Q_j))$ unless every element of that class centralizes $O_p(N_G(Q_j))$. Thus when $a_{ij}^{(k)} \neq 0$, we have $K_i\tau s' \neq 0$ and $K_k\tau \neq 0$, so that $Q_j \lesssim Q_k$, $K_i\tau$ involves an element which centralizes $O_p(N_G(Q_j))$, and hence $O_p(N_G(Q_j)) \lesssim Q_i$ also.

Proof of Theorem 3. Using the argument of Lemma 4 (or a slight variation of the proof of the main theorem of [1]), it can be seen that $K_i s = \sum_{j=1}^{r} s_{ij} K_j$ for $1 \leqslant i \leqslant n$. We saw during the course of the proof of Theorem 1 that if $s_{ij} \neq 0$ and $|Q_j| = |Q_i|$, then Q_i is a defect group for some p-block of G. Suppose, on the other hand, that Q_i is a defect group for some p-block of G. Then Q_i is a defect group for some p-block of $N_G(Q_i)$ also.

Let τ denote the Brauer homomorphism from $Z(FG)$ to $Z(FN_G(Q_i))$. We note that if Q_j is conjugate to Q_i, then s_{ij} is the coefficient of $K_j\tau$ in $(K_i\tau)s'$ (where s' is the obvious analogue of the map s). By the main theorem of [1], as Q_i is a defect group for some p-block of $N_G(Q_i)$, there is some k such that y_k is distinguished, Q_k is conjugate to Q_i, and $s_{kj} \neq 0$ for some j such that $|Q_j| = |Q_k|$ (we essentially proved this during the course of the proof of Theorem 1).

We know that $s_{ij} = 0$ unless $Q_j \lesssim Q_i$. Thus, if in the matrix $S(D)$ the entries s_{kj} and s_{jk} are both non-zero, then Q_k and Q_j are conjugate in G, and

both are defect groups for some p-block of G. Furthermore, if Q_i is a defect group for some p-block of G, then there is a pair $\{j, k\}$ such that $s_{kj} \neq 0$, $s_{jk} \neq 0$, and Q_k is conjugate to Q_i. Hence the p-subgroups of G which are defect groups for p-blocks of G, and are contained up to conjugacy in D, are precisely those Q_k such that $k \leqslant n$ and, for some $j \leqslant r$, $s_{jk}s_{kj} \neq 0$. In particular, a knowledge of the matrix $S(D)$ determines which subgroups of D are defect groups for p-blocks of G.

(ii) We have seen that $\{K_i s: 1 \leqslant i \leqslant n\}$ spans $I(D)s$. From the matrix $S(D)$, for $1 \leqslant j \leqslant n$, we know that $K_j s = \sum_{k=1}^{r} s_{jk} K_k$. Thus for $1 \leqslant i, j \leqslant n$, $(K_i s)(K_j s) = \sum_{k=1}^{r} s_{jk}(K_i s)K_k$. From the matrix $A(D)$, we know that $(K_i s)K_k = \sum_{l=1}^{r} a_{il}^{(k)} K_l$. Hence, from a knowledge of $A(D)$ and $S(D)$ (and how they are labelled), we can determine all products $(K_i s)(K_j s)$ for $1 \leqslant i, j \leqslant n$. Consequently, we can determine the multiplication within the algebra $I(D)s$, which is a semi-simple algebra with a unit element (or else is already 0). From this knowledge, we can recover the primitive idempotents of $I(D)s$, which are precisely the block idempotents of the p-blocks of G whose defect groups are contained in D (more will be said about this in a moment).

Suppose that e is a primitive idempotent of $Z(FG)$ contained within $I(D)s$. Then we may write $e = \sum_{i=1}^{n} \mu_i (K_i s)$, where each $\mu_i \in F$. We saw in the proof of Theorem 1 that $\dim_F(eI^*(D))$ is the number of modular irreducible characters in the p-block of e.

For $1 \leqslant k \leqslant r$, $eK_k = \sum_{i=1}^{n} \mu_i (K_i s)K_k = \sum_{i=1}^{n} \mu_i \sum_{j=1}^{r} a_{ij}^{(k)} K_j$. Thus, letting U denote the n-long row vector with ith entry μ_i, we see easily that the number of modular irreducible characters in the p-block of e is the rank of the $r \times r$ matrix whose kth row is $UA^{(k)}$.

2. Decomposing Semi-simple Algebras

In this section we make the following assumptions: A is a finite-dimensional, semi-simple, commutative algebra with a unit element, over the finite field F (the arguments we give can be slightly modified if F is not finite). A has the basis $\{a_1, a_2, \ldots, a_n\}$, and we are given the class algebra constants $\lambda_{ijk} \in F$ such that $a_i a_j = \sum_{k=1}^{n} \lambda_{ijk} a_k$. We suppose that F has q-elements.

We first claim that $A \otimes_F F_1$ is a direct sum of one dimensional subalgebras, where F_1 has q^r elements and r is the smallest integer such that $a_i^{q^r} = a_i$ for $1 \leqslant i \leqslant n$ (and that F_1 is the smallest field containing F which has this property).

Let F^* be an extension of F such that $A \otimes_F F^*$ contains n mutually orthogonal idempotents, say $e_1, \ldots, e_n$. Then there are elements $\mu_{ij} \in F^*$ such that $a_i = \sum_{j=1}^{n} \mu_{ij} e_j$ for $1 \leqslant i \leqslant n$. Since $a_i^{q^r} = a_i$ for each i, $\mu_{ij}^{q^r} = \mu_{ij}$ for all i

and j. Hence we may suppose that F^* is an extension of F_1 (as F_1 has q^r elements), and that $\mu_{ij} \in F_1$ for all i, j. Let U be the $n \times n$ matrix $[\mu_{ij}]$. Then for $1 \leqslant i \leqslant n$, $e_i = \sum_{j=1}^{n} \gamma_{ij} a_j$, where γ_{ij} is the i, j entry of the matrix U^{-1}. In particular, each e_i lies in $A \otimes_F F_1$, and both our claims are established. (We remark that we can define an $n \times n$ matrix $T = [t_{ij}]$, with entries in F such that $a_i^q = \sum_{j=1}^{n} t_{ij} a_j$ for each i, and that r is the smallest natural number such that $T^r = I$.)

Our next task is to identify 1_A. There are several ways to do this, and we mention one systematic, but tedious, way. For $1 \leqslant i \leqslant n$, let $b_i = a_i^{q^r - 1}$. Then $b_i^2 = b_i$ for each i, and $b_i \neq 0$ for any i. We define idempotents f_i inductively as follows: $f_1 = b_1$; $f_k = f_{k-1} + (b_k - f_{k-1} b_k)$ for $2 \leqslant k \leqslant n$.

We claim that, for each k, we have $a_i f_k = a_i$ for $1 \leqslant i \leqslant k$. When $k = 1$, we have $a_1 f_1 = a_1 b_1 = a_1 a_1^{q^r - 1} = a_1^{q^r} = a_1$. Suppose that for some j, we have $a_i f_j = a_i$ for $1 \leqslant i \leqslant j$. Then for $1 \leqslant i \leqslant j$, $a_i f_{j+1} = a_i f_j + a_i(b_{j+1} - f_j b_{j+1}) = a_i f_j = a_i$. Also, $a_{j+1} f_{j+1} = a_{j+1} f_j + a_{j+1} b_{j+1} - a_{j+1} b_{j+1} f_j$. Now $a_{j+1} b_{j+1} = a_{j+1}^{q^r} = a_{j+1}$, so that $a_{j+1} f_{j+1} = a_{j+1}$. Hence our claim is established. In particular, $a_i f_n = a_i$ for $1 \leqslant i \leqslant n$, so that $f_n = 1_A$.

We now describe a systematic method of finding the primitive idempotents of $A \otimes_F F_1$. To minimize the confusion caused by notation, we assume from now on that $F_1 = F$ and that $r = 1$.

For each $x \in A$, and $\lambda \in F^{\#}$, we let $E_\lambda(x) = -\sum_{i=1}^{q-1} (\lambda^{-1} x)^i$. Since $(\lambda^{-1} x)^q = \lambda^{-1} x$, it readily follows that $E_\lambda(x)^2 = E_\lambda(x)$. Also, for any x we see easily that $E_\lambda(x) E_\mu(x) = 0$ for $\lambda \neq \mu$ in F. We let $E_0(x) = 1_A - \sum_{\lambda \in F^{\#}} E_\lambda(x)$ for each $x \in A$. Then for each $x \in A$, $E_0(x) + \sum_{\lambda \in F^{\#}} E_\lambda(x)$ gives a decomposition of 1_A as a sum of mutually orthogonal idempotents (neglecting those λ for which $E_\lambda(x) = 0$).

It is not difficult to verify that $x = \sum_{\lambda \in F^{\#}} \lambda E_\lambda(x)$, and $E_\lambda(x) \neq 0$ iff λ is a root of the minimum polynomial of x over F (including the case $\lambda = 0$). The key to finding the primitive idempotents of A is:

LEMMA 5. *Let e be a primitive idempotent of A. Then there is a unique n-tuple $(\lambda_1, \lambda_2, \ldots, \lambda_n)$ of elements of F such that $e = \prod_{i=1}^{n} E_{\lambda_i}(a_i)$. Any product of the latter form is 0 or a primitive idempotent of A.*

Proof. For $1 \leqslant i \leqslant n$, we may write $1_A = \sum_{\lambda \in F} E_\lambda(a_i)$. We may multiply these n decompositions of 1_A, together to obtain an orthogonal decomposition of 1_A, where each term has the form $E_{\mu_1}(a_1) \cdots E_{\mu_n}(a_n)$ (for different n-tuples gives rise to orthogonal terms). As e is a primitive idempotent, there is an n-tuple $(\lambda_1, \ldots, \lambda_n)$ such that $e = e \prod_{i=1}^{n} E_{\lambda_i}(a_i)$. We claim that $e = \prod_{i=1}^{n} E_{\lambda_i}(a_i)$, and it follows from our remarks above that the n-tuple $(\lambda_1, \ldots, \lambda_n)$ is unique.

We prove by induction on $\dim_F(A)$ that for any n-tuple $(\mu_1, \ldots, \mu_n)$ of elements of F, $\prod_{i=1}^{n} E_{\mu_i}(a_i)$ is either 0 or a primitive idempotent of A.

Suppose that $\prod_{i=1}^{n} E_{\mu_i}(a_i) \neq 0$. Our assertion is certainly true when $n = 1$, so we can assume that a_1 is not a multiple of 1_A, in which case $E_{\mu_1}(a_1) \neq 1_A$. Let $z = E_{\mu_1}(a_1)$, so $z^2 = z \neq 0$.

For $2 \leqslant i \leqslant n$, we have $E_{\mu_i}(a_i z) = zE_{\mu_i}(a_i)$. Hence $\prod_{i=1}^{n} E_{\mu_i}(a_i) = \prod_{i=1}^{n} E_{\mu_i}(a_i z)$. Now $\dim_F(Az) < \dim_F(A)$, Az is a semi-simple commutative algebra with unit element z, and is spanned by $a_1 z, a_2 z, \ldots, a_n z$. By induction, $\prod_{i=1}^{n} E_{\mu_i}(a_i z)$ is a primitive idempotent of Az (in fact, some proper subproduct of it is already a primitive idempotent, as a proper subset of $\{a_1 z, \ldots, a_n z\}$ spans Az). Thus $\prod_{i=1}^{n} E_{\mu_i}(a_i)$ is a primitive idempotent of A, as claimed. Hence $\prod_{i=1}^{n} E_{\lambda_i}(a_i)$ is a primitive idempotent of A, and as $e \prod_{i=1}^{n} E_{\lambda_i}(a_i) = e$, we must have $\prod_{i=1}^{n} E_{\lambda_i}(a_i) = e$.

Remark. Examination of the arguments we have used reveals that it is only necessary to assume that $\{a_i : 1 \leqslant i \leqslant n\}$ spans A. A little more thought reveals that it is only necessary to assume that $\{a_i : 1 \leqslant i \leqslant n\}$ generates A *as an algebra.*

We also remark that the method we have outlined can be made quite efficient computationally, as follows: for $1 \leqslant k \leqslant n$, each k-tuple $(\mu_1, \ldots, \mu_k)$ gives an element $\prod_{i=1}^{k} E_{\mu_i}(a_i)$, which is either idempotent or 0. Any two distinct k-tuples give rise to elements whose products are 0. As $\dim_F(A) = n$, there are at most n k-tuples $(\mu_1, \mu_2, \ldots, \mu_n)$ such that $\prod_{i=1}^{k} E_{\mu_i}(a_i) \neq 0$ (in fact, if there are n, these are all primitive idempotents of A). We can multiply each of these "survivors" at stage k in turn by each $E_\lambda(a_{k+1})$ as λ ranges through F to determine the "survivors" at stage $k+1$. At each stage, we have to perform at most nq multiplications of elements of A. The "survivors" at stage n are all primitive idempotents of A, and we can obtain these by performing something of the order of qn^2 multiplications of elements of A.

Returning to the situation of Theorem 3, from a knowledge of the matrix $S(D)$ we can refine $\{K_i s : 1 \leqslant i \leqslant n\}$ to a basis for $I(D)s$ (for example, we could use Gaussian elimination). Let $A = I(D)s$. Then we may regard A as a semi-simple commutative algebra with unit element (unless $A = 0$ already) over $GF(p)$. From the matrices $A(D)$ and $S(D)$, as we have described already, we can determine all products of elements of the basis found above. We can then follow the procedures outlined above to find a splitting field, F_1, for A, and find the primitive idempotents of $A \otimes_{GF(p)} F_1$. Thus we do not even need to know $|G|_{p'}$, or to be given a splitting field of characteristic p for G, for the matrices $S(D)$ and $A(D)$ contain all the necessary information to decompose $I(D)s$. (Some, or all, of the results of this section are well-known, no doubt).

3. Double Coset Decompositions

In this section, we illustrate how the numbers $a_{ij}^{(k)}$ are determined by the way in which conjugates of y_i and y_j are distributed among the cosets of Q_k in G.

For $1 \leqslant k \leqslant r$, we pick a full set of (Q_k, Q_k)-double coset representatives say $\{g_i : 1 \leqslant i \leqslant t\}$, chosen whenever possible so that g_i is p-regular and g_i centralizes $Q_k \cap Q_k^{g_i}$. We label so that g_i satisfies the stated condition for $i \leqslant b$, but g_i does not when $i > b$. If $b = 0$, we set $B^{(k)} = [0]$ $(n \times r)$. Otherwise, we set $B^{(k)} = M^{(k)} N^{(k)T}$, where $M^{(k)}$ is the $n \times b$ matrix whose (i, j)-entry, $m_{ij}^{(k)}$, is the residue (mod p) of the number of conjugates of y_i in $g_j C_{Q_k}(Q_k \cap Q_k^{g_j})$, and where $N^{(k)}$ is the $r \times b$ matrix whose (i, j) entry, $n_{ij}^{(k)}$, is the residue (mod p) of the number of orbits which $Q_k \cap Q_k^{g_j}$ has on conjugates of y_i in $g_j y_k Q_k$ whose centralizers have a Sylow p-subgroup contained in Q_k.

We define the $nr \times r$ matrix $B(D)$ to have its $(tn + i)$th row equal to the ith row of $B^{(t+1)}$ for $0 \leqslant t \leqslant r - 1$, $1 \leqslant i \leqslant n$.

THEOREM 5. *For* $1 \leqslant j,\ k \leqslant r,\ 1 \leqslant i \leqslant n,\ a_{ij}^{(k)} = (|C_G(y_j)|_{p'}^*/|C_G(y_k)|_{p'}^*)$ $b_{ij}^{(k)}$. *In particular, the matrices* $A(D)$ *and* $B(D)$ *have the same rank.*

Proof. We calculate the contribution to $|\Omega_{ij}^{(k)}|$ from the double cosets $Q_k g Q_k$ and $Q_k h y_k Q_k$, for $g, h \in G$. We may suppose that $h^{-1} g y_k \in y_k Q_k$, so that $h^{-1} g \in Q_k$, and $g \in h Q_k$. Hence we may suppose that $g = h$.

For $u \in Q_k$, the contribution to $|\Omega_{ij}^{(k)}|$ from gQ_k and $gy_k Q_k$ is the same as that from ugQ_k and $ugy_k Q_k$, for if $a \in gQ_k$ and $b \in gy_k Q_k$ with $(a, b) \in \Omega_{ij}^{(k)}$, then $uau^{-1} \in ugQ_k$, $ubu^{-1} \in ugy_k Q_k$ and $(uau^{-1})^{-1}(ubu^{-1}) \in y_k Q_k$ (similarly, if $x \in ugQ_k$, $y \in ugy_k Q_k$, and $(x, y) \in \Omega_{ij}^{(k)}$, then $(u^{-1}xu, u^{-1}yu) \in \Omega_{ij}^{(k)}$, and $u^{-1}xu \in gQ_k$, $u^{-1}yu \in gy_k Q_k$).

Hence the contribution we seek is $[Q_k : Q_k \cap gQ_k g^{-1}]$ times the contribution from gQ_k and $gy_k Q_k$. We note that $Q_k \cap gQ_k g^{-1}$ permutes the conjugates of y_i within gQ_k, and that $Q_k \cap (gy_k)Q_k(gy_k)^{-1}$ permutes the conjugates of y_j within $gy_k Q_k$. As $y_k \in C_G(Q_k)$, we see easily that $Q_k \cap gQ_k g^{-1} = Q_k \cap (gy_k)Q_k(gy_k)^{-1}$.

The contribution to $|\Omega_{ij}^{(k)}|$ from gQ_k and $gy_k Q_k$ is

$$\sum_{\alpha,\beta} [Q_k \cap gQ_k g^{-1} : Q_k \cap gQ_k g^{-1} \cap C_G(z_\alpha)] \times [Q_k \cap gQ_k g^{-1} : Q_k \cap gQ_k g^{-1} \cap C_G(w_\beta)]$$

as z_α, w_β range respectively through orbit representatives of the orbits which $Q_k \cap gQ_k g^{-1}$ has on conjugates of y_i within gQ_k and conjugates of y_j within $gy_k Q_k$.

Hence, the contribution to $|\Omega_{ij}^{(k)}|$ from $Q_k g Q_k$ and $Q_k g y_k Q_k$ is

$$\sum_{\alpha,\beta} [Q_k : Q_k \cap gQ_k g^{-1} \cap C_G(w_\beta)][Q_k \cap gQ_k g^{-1} : Q_k \cap gQ_k g^{-1} \cap C_G(z_\alpha)].$$

However, our real concern is $a_{ij}^{(k)}$, which is the residue (mod p) of $(|C_G(y_j)|/|C_G(y_k)|)|\Omega_{ij}^{(k)}|$. The term

$$\frac{|C_G(y_j)|}{|C_G(y_k)|}[Q_k : Q_k \cap gQ_k g^{-1} \cap C_G(w_\beta)] \times [Q_k \cap gQ_k g^{-1} : Q_k \cap gQ_k g^{-1} \cap C_G(z_\alpha)]$$

makes no contribution to this residue unless $Q_k \cap gQ_k g^{-1} \cap C_G(w_\beta) \in \mathrm{Sylp}(C_G(w_\beta))$ and $Q_k \cap gQ_k g^{-1} \subseteq C_G(z_\alpha)$ (for w_β is conjugate to y_j). If both conditions are satisfied, the contribution to the residue is $|C_G(y_j)|_{p'}^*/|C_G(y_k)|_{p'}^*$.

The total contribution to $a_{ij}^{(k)}$ from these double cosets is $|C_G(y_j)|_{p'}^*/|C_G(y_k)|_{p'}^* m_i(g)^* n_j(g)^*$, where $m_i(g)$ is the number of conjugates of y_i within gQ_k which centralize $Q_k \cap gQ_k g^{-1}$, and $n_j(g)$ is the number of orbits which $Q_k \cap gQ_k g^{-1}$ has on conjugates of y_j within $gy_k Q_k$ whose centralizers have a Sylow p-subgroup contained in Q_k (hence in $Q_k \cap gQ_k g^{-1}$).

We may suppose then that g is conjugate to y_i and that g centralizes $Q_k \cap gQ_k g^{-1}$ (in which case, $Q_k \cap gQ_k g^{-1} = Q_k \cap Q_k^g$). Hence we may suppose that $g = g_l$ for some $l \leqslant b$. Consequently, we obtain

$$a_{ij}^{(k)} = \frac{|C_G(y_j)|_{p'}^*}{|C_G(y_k)|_{p'}^*} \sum_{l=1}^{b} m_{il}^{(k)} n_{jl}^{(k)} = \frac{|C_G(y_j)|_{p'}^*}{|C_G(y_k)|_{p'}^*} (M^{(k)} N^{(k)T})_{ij} = \frac{|C_G(y_j)|_{p'}^*}{|C_G(y_k)|_{p'}^*} b_{ij}^{(k)},$$

as claimed. The proof of Theorem 5 is complete.

Acknowledgments

I wish to thank Dr. J. Olsson, as he suggested to me in October 1982 that it might be possible to prove an analogue of the main theorem of [1], in which information about the number of modular irreducible characters in certain p-blocks could be obtained. It was this suggestion that inspired me to attempt to generalize the methods of [1] to this case.

Reference

1. G. R. Robinson, The number of blocks with a given defect group, *J. Algebra* **84** (1983), 493–502.